

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of

Implementation of the Telecommunications Act of 1996; CC Docket No. 96-115

Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information;

Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information RM-11277

COMMENTS OF NEXTG NETWORKS, INC.

NextG Networks, Inc., on behalf of its operating subsidiaries (collectively "NextG")¹, submits the following comments in response to the Commission's Notice of Proposed Rulemaking to address concerns raised by the Electronic Privacy Information Center ("EPIC") concerning customer proprietary network information ("CPNI").²

¹ The NextG operating subsidiaries joining in these comments are: NextG Networks of NY, Inc., NextG Networks Atlantic, Inc., NextG Networks of California, Inc. and NextG Networks of Illinois, Inc.

² *In Re Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, Notice of Proposed Rulemaking, 21 FCC Rcd 1782 (FCC rel. Feb. 14, 2006) (hereinafter "NPRM"). The NPRM was prompted at least in part by a petition for rulemaking filed by EPIC. *In Re Implementation of the Telecommunications Act of 1996*, Petition of the Electronic Privacy Information Center for Rulemaking to Enhance and Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (hereinafter "EPIC Petition").

I. INTRODUCTION AND SUMMARY

There has been much publicity recently about unauthorized access to customer phone records, a practice often called “pretexting.” Pretexting involves data brokers who gather personal information about end user customers of telecommunications services, such as the Internet, then use that information to contact the end user’s carrier and pretend to be the end user in order to harvest customer proprietary network information (“CPNI”). NextG appreciates the Commission’s concern with the problem of pretexting. However, as discussed in these comments, NextG is concerned that the application of the Commission’s proposed and even existing CPNI rules and regulations needs to be more carefully defined. It appears that the proposed rules would impose obligations on NextG, which is a carriers’ carrier, despite the fact that the proposed rules were intended to protect CPNI for retail end users. Without addressing the merits of the proposed rules, NextG submits that the Commission should recognize that the rules should not apply to a carrier’s carrier, like NextG, which has no access to retail end user CPNI.

It does not appear that the Commission, in its orders promulgating the current CPNI rules (47 C.F.R. §§ 64.2001 *et seq.*, hereinafter “rules”), was concerned about, addressed, or considered the handling of customer information of the kind retained by NextG. Moreover, the underlying policy concern of 47 U.S.C. § 222 (“Section 222”) and the rules—protecting retail end users’ personal information—is not implicated in a service such as NextG’s. Yet, in response EPIC’s Petition, the Commission is now considering whether to adopt additional CPNI rules. Unfortunately, the proposed rules again appear to have forgotten carrier’s carriers, like NextG. They appear to apply to any telecommunications provider, regardless of whether the provider has access to any end

user CPNI. Application of the proposed CPNI rules to NextG would be unduly burdensome, inappropriate, and ultimately with no positive effect. As such, NextG respectfully requests that the Commission decline to adopt the rules as proposed. Alternatively, should the Commission adopt any of the rules proposed by EPIC, NextG submits that the Commission should clarify that Section 222 and the current and new rules do not apply to a service such as NextG's RF Transport Service, or that it amend its rules to specifically exempt carrier's carriers with no access to end user CPNI from Section 222 and the rules (both current and any new rules).

II. NEXTG'S SERVICE AND ITS ACCESS TO CPNI

NextG is a "carrier's carrier." It provides transport and backhaul services of voice and data signals primarily for wireless carriers. NextG's "RF Transport" services provide these wireless carriers with custom solutions to enhance the efficiency and capacity of their networks, strictly in a carrier's carrier capacity. While NextG has tariffs on file in a number of states, in most cases, NextG's carrier customers buy bulk transport for individually-negotiated prices, terms and conditions, depending on anticipated usage, technical requirements, location, etc. Thus, while NextG necessarily obtains information regarding the quantity, technical configuration, location, etc. of the telecommunications services provided to NextG's customers, it has no access to CPNI related to end user customers.

While "retail" users who subscribe to the wireless services of NextG's customers ultimately benefit from the enhanced network capacity and coverage afforded to the carriers by NextG, NextG's network and services are transparent to them. NextG has no customer relationship with those retail users, and most importantly, no *retail end user* CPNI is transferred to or available to NextG. Rather, NextG only has access to

information regarding *NextG's customers*—i.e., the wireless carriers themselves. This information includes bulk capacity used, technical configuration of the wireless network, location of the interconnection points of the two networks, etc. Once a wireless carrier becomes a NextG customer, NextG has access to this information and may use it to suggest modifications, expansions or upgrades of the existing or future service. Indeed, NextG and its customers typically work closely together in the engineering of node locations and other such network and service configuration issues.

III. THE POLICY CONCERN UNDERLYING THE CPNI RULES IS NOT IMPLICATED BY A SERVICE SUCH AS NEXTG'S

The CPNI rules embodied in Section 222 of the Communications Act and Commission rules grew out of legislation introduced in 1993 seeking to protect “residential consumers and . . . small businesses.”³ The concerns being addressed by the proposed legislation were services such as caller ID and 800/900 services wherein carriers were divulging residential and small business end user telephone numbers. This proposed legislation was the first iteration of what eventually evolved into Section 222 of the Act (47 U.S.C. § 222). Commission orders promulgating rules under Section 222 were similarly concerned with the information of end users, whether accessed directly by the end user’s carrier or its affiliate, or indirectly through a wholesale relationship between the end user’s carrier and another carrier leasing facilities to the end user’s carrier.⁴ In enacting Section 222 and promulgating the CPNI rules, neither the Commission nor

³ *Extension of Remarks of Edward J. Markey*, 139 Cong. Rec. E2745-01.

⁴ See discussion of accessing CPNI through wholesale arrangements in *In Re Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409 (FCC rel. Sept. 3, 1999).

Congress were concerned with protecting information concerning the quantity, technical configuration, location, etc. of telecommunications services purchased on a bulk basis by telecommunications carriers from "carriers' carriers." Nor should they have been so concerned. Carrier's carriers, like NextG, have no access to end user CPNI. Moreover, NextG's customers are major wireless and CMRS carriers that have ample resources and are sufficiently sophisticated in business generally and the telecommunications industry specifically to fully protect their privacy interests. To illustrate, NextG has negotiated and executed nondisclosure agreements with all of its customers, which address the customer's individual privacy preferences.⁵ Unlike in the end user context, there is no consumer protection need present when the telecommunications service customers are major CMRS or other wireless carriers buying high capacity transport services.

IV. THE PROPOSED RULES WOULD BE INAPPROPRIATE FOR A CARRIER'S CARRIER, LIKE NEXTG, WITH NO DIRECT OR INDIRECT ACCESS TO END USER CPNI

Although NextG could find no instance of the CPNI rules being enforced against a carrier providing a service similar to its RF Transport service, the language of Section 222 and the CPNI rules is written broadly enough that it seemingly encompasses all telecommunications carriers, without specifically limiting the application of those rules to those with access to the CPNI of retail end users. It is unclear, however, whether the rules actually apply to NextG or not, and as such, NextG's operating subsidiaries filed their CPNI certifications with the Commission on February 6, 2006. The only potentially

⁵ For further description of NextG's CPNI policies and practices, see the CPNI certifications filed by the operating subsidiaries listed in note 1 above, filed with the Commission on February 6, 2006. These certifications were filed pursuant to the Public Notice issued by the Enforcement Bureau on Jan. 30, 2006, DA 06-223.

relevant discussion in the Commission's orders is a statement that it should not, at the time of that rulemaking proceeding (*i.e.*, 1998), "distinguish among carriers for the purpose of applying section 222(c)(1)" and that Section 222 applies to all carriers.⁶ This language, however, was written in response to requests from commenters participating in that rulemaking that the Commission impose less stringent rules on new entrants and/or non-dominant carriers—not that the application of the rules be limited to protecting retail end users' CPNI. Thus, it is not clear that the existing rules even apply to NextG.⁷

The Commission now seeks comment on proposed additional CPNI rules. Setting aside the question of whether they will be effective, in any case, the proposed rules would be inappropriate for and unduly burdensome to NextG and others like it. For example, EPIC has proposed that carriers be required to encrypt stored CPNI data.⁸ Such a measure is certainly unjustified in the context of NextG's business, which involves a limited number of large business accounts and no information regarding individual end users. Not only are there fewer customer accounts to deal with, but NextG's accounts are handled by high-level sales personnel intimately familiar with each account—not by customer call centers handling thousands of accounts per day as in the context of residential/small business customers. The risk of an erroneous release, therefore, is nonexistent or negligible. NextG also has a strong business incentive not to reveal private information regarding its customers' networks, or the custom solutions and pricing established for any particular customer. Revealing this information publicly

⁶ *In Re Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (FCC rel. Feb. 26, 1998) at ¶ 49.

⁷ If they do, NextG clearly complies with the current rules, as was demonstrated in NextG's recent CPNI certification filings.

⁸ EPIC Petition at 11; NPRM at ¶ 19.

would have a significantly negative impact on NextG's ability to attract and maintain current customers, and would give NextG's competitors damaging insight into how NextG formulates its service offerings and pricing. Clearly, requiring NextG to engage in expensive upgrades to its computer systems to encrypt customer information is unwarranted and unduly burdensome in NextG's case.

The Commission also has asked for comment on EPIC's proposal that carriers be required to use consumer-set passwords and keep an "audit trail" to record all instances where a customer's record is accessed.⁹ Imposing password and audit trail requirements on NextG would be quite burdensome and would yield no benefit. As explained above, NextG has large customers that are relatively few in number compared to carriers serving retail end users that are the target of the CPNI rules and the present proceeding. NextG's customers are not "anonymous" to the customer relations personnel at NextG the way that thousands of individual home telephone customers might be to an ILEC. NextG's customers have designated high-level operational and business contact personnel for purposes of managing their accounts with NextG, and NextG personnel are in frequent contact with such personnel. Each party is familiar with the people authorized to receive customer account information and the specific types of information each person is authorized to access. NextG is also contractually bound not to release customer information to persons not authorized by the customer to discuss its NextG account. Routine business correspondence provides more than an ample "trail" of the customer information exchanged between NextG and its customers. Imposing password and audit trail requirements on NextG, therefore, would provide absolutely no benefit to NextG's customers and would be a burdensome annoyance to both NextG and its customers.

⁹ EPIC Petition at 11; NPRM at ¶¶ 15, 17.

Finally, EPIC suggests that carriers destroy older customer records when no longer needed for billing or dispute purposes.¹⁰ Again, such a requirement is not necessary or appropriate for, and would be extremely harmful to NextG's business. NextG builds custom networks designed for customers to use over the course of multiple decades. For a variety of operational, tax and general prudent business practice reasons, NextG must retain its customer account records well beyond the period needed for more immediate billing and dispute resolution purposes. In addition, NextG vigilantly safeguards its customers' records because it is contractually obligated and has a strong business interest in doing so. Unauthorized release of its customers' records would be devastating to NextG's business because the people most interested in accessing such records are its customers' competitors and moreover NextG's competitors. Any such unauthorized release would likely be subject to legal action and would cost NextG current and potential customers. The imposition of a requirement to destroy older customer records on NextG would not only be extremely harmful but completely unnecessary.

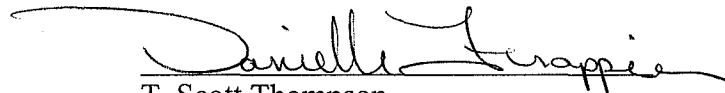
V. CONCLUSION

Given that previous Commission orders have not directly addressed the issue of carrier's carriers with no access to end user CPNI, that imposing Section 222 and the current or proposed rules would not serve the underlying policy goals of the statute, and that imposing the proposed new CPNI rules on NextG would be unduly burdensome and serve no useful purpose, NextG respectfully requests that the Commission clarify that neither Section 222 nor its CPNI rules at 64.2001 *et seq.* (and any amendments to those rules) apply to carriers that have no direct or indirect access to end user CPNI, such as

¹⁰ EPIC Petition at 11-12; NPRM at ¶ 20.

NextG. Alternatively, if the Commission finds that a simple clarification is not possible, NextG urges the Commission to amend its rules to exempt such carriers from Section 222 and the CPNI rules, both current and proposed. At a minimum, NextG submits that the Commission should more carefully tailor any new CPNI rules to avoid imposing on carriers, like NextG, obligations that while perhaps appropriate for providers serving retail, residential end users are unrealistic and unnecessary for carriers serving only other carriers with no access to end user CPNI.

Respectfully submitted,



T. Scott Thompson
Danielle Frappier
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Ave., N.W., Suite 200
Washington, D.C. 20006
(202) 659-9750
sthompson@crblaw.com
dfrappier@crblaw.com

Robert L. Delsman
NextG Networks, Inc.
2216 O'Toole Ave.
San Jose, CA, 95131
(408) 954-1580
rdelsman@nextgnetworks.net

Counsel for NextG Networks, Inc.

April 28, 2006